| | |
|---|---|
| Date of issue of the regulation | 05/10/2020 |
| Effective date of the regulation | 01/05/2021 |
| In effect | Until further notice |
| Legal basis | Act on the Secondary Use of Health and Social Data (552/2019), section 22(3) and section 24(2) (in the regulation referred to as the “Act on Secondary Use”) |

# Regulation by the Health and Social Data Permit Authority: Requirements for other service providers' secure operating environments

## 1 Background

The Health and Social Data Permit Authority Findata (hereinafter “data permit authority”) maintains a secure operating environment in accordance with section 20(1) of the Act on Secondary Use. The data sets for which the data permit authority has granted a permit for use are, as a rule, disclosed for processing by the permit holder in the operating environment in question.

If the data permit application requests that data sets be disclosed for processing in another operating environment than the data permit authority’s secure operating environment, the application must, according to section 20(3) of the Act on Secondary Use, separately state reasons why this is absolutely necessary. In such a case, the data permit authority or another authority referred to in this Act on Secondary Use may disclose the data to the applicant only if the operating environment meets the conditions laid down in section 20(2) and sections 21–29.

If an individual controller referred to in section 44(3) of the Act on Secondary Use has made a decision on a data permit concerning data included in its own registers, it must always disclose the data sets for processing by the permit holder in the secure operating environment referred to in section 20 of the Act on Secondary Use.

According to section 24(2) of the Act on Secondary Use, the data permit authority will issue further provisions on the requirements concerning secure operating environments of other service providers. The requirements must require the same level of data security as is required for the data permit authority's own operating environment.

Before the regulation entered into effect, a round for comments was organised from 22 May to 26 June 2020, during which a total of 54 comments were submitted. These comments were taken into account in the preparation of the regulation.

The requirements for a secure operating environment are included as Annex 1 to this regulation.

## 2 Scope of the regulation

This regulation is the data permit authority’s provision on the requirements concerning secure operating environments of other service providers, referred to in section 24(2) of the Act on Secondary Use.

This provision applies to all purposes laid down in the Act on Secondary Use for which a data permit is required under the Act on Secondary Use. These purposes include scientific research, statistics, teaching and the planning and investigation tasks of the authorities. With regard to teaching, the regulation pertains to the preparation of teaching materials, not actual teaching.

Implementation of the requirements laid down in this regulation is a prerequisite for the data permit authority to consider and disclose data sets for processing by the permit holder in an operating environment other than its own as of 1 May 2021.

The fulfilment of the requirements of this requirement will be verified by means of a certificate issued by an information security inspection body. Provisions on the inspection of information security are laid down in section 26 of the Act on Secondary Use.

## 3 Validity of the regulation and amendments

This regulation is in effect until further notice.

## 4 Applicable legislation

Act on the Secondary Use of Health and Social Data (552/2019), sections 18–34, section 60(1).

Seppänen Johanna 912110564

Digitaalinen allekirjoittaja: Seppänen Johanna 912110564
Hakemistonimi (DN): c=FI, o=Terveyden ja hyvinvoinnin laitos, serialNumber=912110564, givenName=Johanna, sn=Seppänen, cn=Seppänen Johanna 912110564
Päiväys: 2020.10.23 14:24:29 +03'00'

Johanna Seppänen
Director

Lanu Heikki 91215375E

Digitaalinen allekirjoittaja: Lanu Heikki 91215375E
Hakemistonimi (DN): c=FI, o=Terveyden ja hyvinvoinnin laitos, serialNumber=91215375E, givenName=Heikki, sn=Lanu, cn=Lanu Heikki 91215375E
Päiväys: 2020.10.23 13:32:23 +03'00'

Heikki Lanu
Head of ICT

This regulation has been signed electronically.

# Annex 1: Requirements for a Secure Operating Environment

## Contents

# 1 General information

This document describes and specifies the information security requirements for the secure operating environment required by the Act on Secondary Use (Act on the Secondary Use of Social and Health Data, 552/2019). The service provider is required to comply with the general data security requirements laid down in section 18. A secure operating environment ensures the secure processing of data disclosed under the Act on Secondary Use in accordance with the permit. The authority may disclose the data sets to the applicant only if the operating environment meets the conditions laid down in section 20(2) and sections 21–29.

Information security requirements aim to ensure that the service provider of a secure operating environment has sufficient security arrangements to prevent the unlawful disclosure of confidential information. This regulation does not take a stand on technical implementation, and therefore requirements need to be examined on a case-by-case basis.

The information security inspection body carrying out the inspections and issuing the certificate assesses, with its own professional competence, whether the valid information security certificates concerning the secure environment are suitable for meeting the requirements laid down in the regulation. The data permit authority does not carry out an assessment or provide technical advice related to the information security of a secure operating environment.

Information security requirements refer to the following provisions and criteria:

- Act on the Secondary Use of Health and Social Data, 552/2019
- KATAKRI 2015 - Information security audit tool for authorities
    - The KATAKRI Protection level and/or sections in the Example must be taken into account in the application, if any are presented
- PiTuKri version 1 March 2020 - Criteria to Assess the Information Security of Cloud Services
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- ISO/IEC 27001 standard

## 1.1 Definitions

For the purposes of this regulation:

- Material refers to information material containing personal data.

- A physically and technically protected area refers to an environment in which facilities and technical solutions prevent uncontrolled access to information by outsiders. The requirements related to the premises are presented in section 3.3 Premises..

- A quarantine environment refers to a separated and protected solution in which encrypted material is converted into plain language and is subject to an integrity and malware check. In the same environment, the material sent to the data permit authority for inspection is encrypted for delivery. The environment must not be connected to the Internet.

- A user environment refers to a data processing environment, separated on a data permit-specific basis, located in a secure operating environment where a client/researcher or group processes materials containing personal data. The environment must not be directly connected to the Internet or other user environments.

- User and access management refers to a solution that is located between the actual research environment and the Internet and is used to identify users and implement access control.

- Log management refers to a separated and protected solution for the collection, monitoring and reporting of log data in the operating environment.

- Log data includes processing log and disclosure log data as well as technical log data collected by devices in the operating environment.

- Service provider is the party responsible for the operating environment and its compliance, which may also use subcontractors.

- Management of technical, organisational and physical information security refers to management and control solutions for various sections of the implementation of the operating environment.

- The data permit authority's systems refer to information systems managed by the data permit authority, in which, for example, permit processing; and transfer, compilation, pre-processing and combining as well as pseudonymisation and anonymisation of materials are carried out.

- A secure operating environment (hereinafter also operating environment) refers to a technical, organisational and physical operating environment for the processing of data.

- Information security scanning refers to an inspection of the data processing environment carried out using technical aids. This ensures that there are no vulnerabilities or incorrect configurations that endanger information security in the environment.

- An identification source is a system in which the user IDs required for identification and access control are located.

- The principle of least privilege (also the principle of smallest privilege) is a concept related to information security, according to which access rights to an information system must be limited to the narrowest possible rights by which a user or process is able to perform the

task assigned to it. Access rights must also be limited to the shortest possible period of time during which the task can be performed.

## 1.2 Functional description

A secure operating environment refers to a technical, organisational and physical data processing environment in which information security is achieved by appropriate administrative and technical means. In a secure environment, it must be possible to ensure the secure processing of data in accordance with the data permit, and only users identified in the data permit are granted access to the user environment established for the project in question.

The service provider is the operator that provides services of the secure operating environment for the use of its customers. If necessary, the service provider may use subcontractors as suppliers of different components, such as processing and storage capacity. The service provider is responsible for ensuring that the secure operating environment and the parties involved in its provision comply with the requirements laid down in this regulation.

Key functionalities related to a secure operating environment:

- Users log in to the user environment using user IDs of identification sources deemed to be reliable.
- As a rule, two-factor authentication is used when logging in to the user environment.
- In a user environment, the customer only has access to materials specified in the data permit in question.
- If the customer has more than one data permit, they can only process materials from one data permit at a time in a user environment.
- Transfer of personal data sets to a secure environment takes place in a secure manner.
- It should not be possible to establish direct Internet connections in the user environment.
- It must be possible to protect the processing of identifiable personal data sets particularly carefully during all stages of processing.
- Log management must take place in a secure environment that cannot be directly connected to the Internet.

The architecture of the secure operating environment is described below, and the key process steps concerning the service provider are described in section 4.

## 1.3 System architecture

The figure below shows the principal system architecture of a secure operating environment. The purpose is to clarify what functions constitute a secure operating environment and how it is related to other key functions under the Act on Secondary Use.

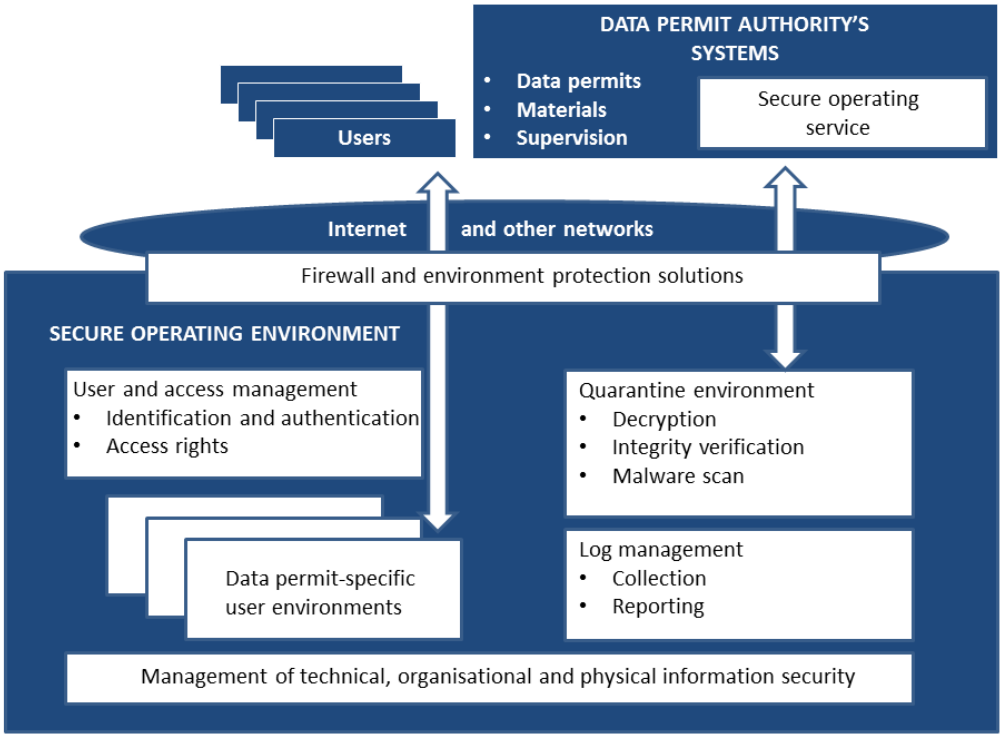


*Figure: Principal system architecture of a secure operating environment*

## 1.4 Service providers

A secure operating environment must have a designated service provider responsible for implementing the requirements of this regulation. The Service Provider may use subcontractors to provide information technology services, for instance, but the service provider is always responsible for the compliance of the secure operating environment. In practice, there must be a binding contractual relationship between the service provider and the subcontractor used.

The service provider must also identify the potential personal data accumulation effect and take this into account in the protection of the operating environment it provides. The accumulation effect may arise, for example, in situations where several personal data sets are to be stored in the operating environment and/or the size of the data sets is large. The National Supervisory Authority for Welfare and Health (Valvira) maintains a public register of compliant operating environments reported to it.

### 1.5 Trusted identification sources

The data permit authority maintains an up-to-date list of the identification sources it trusts and publishes them at www.findata.fi. The service provider may also implement an identification source in connection with its own secure operating environment, which can be regarded as trusted if it meets the requirements of this regulation.

## 2 Technical requirements

### 2.1 Identification

#### 2.1.1 Requirements laid down in the Act on Secondary Use

Section *21 Identifying the users of the secure operating environment*
*https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P21*

#### 2.1.2 Requirements imposed by the data permit authority

1. The initial identification of a user is primarily carried out by means of strong electronic identification, such as the Suomi.fi service. If strong initial electronic identification is not possible, the user's identity must be verified using identity verification documents in the presence of the user in a documented manner. If requiring the user to be present is not reasonable due to travel, for instance, the initial identification can be carried out so that the organisation with an employment, assignment, contractual or similar relationship with the user confirms the user's identity in writing and in a binding manner, with the necessary documents.

2. ID holders and the identification source must have either a contractual relationship (such as an employment or research contract), affiliation (such as through a research project) or other legally binding relationship. Operators of identification sources are obliged to close the identifiers immediately after the contractual relationship has ended, or if they suspect that the identifiers have been leaked or otherwise misused.

3. User identification must have at least two steps, using two different identification methods. In addition to the username-password combination, a separate identifier, such as a mobile phone application or other similar identification method, is used. Two-factor authentication must have taken place before the user begins to process materials according to the data permit.

4. If a terminal device arranged and addressedby the service provider for the user, dedicated for use in the user environment, is located within the same physically and technically protected area as the user environment, two-factor authentication is not required, but the user's identity must be assured before the dedicated terminal device is released for use.

5. In addition to the above, KATAKRI subdivisions I 06 (sections 1–10 in the Example) and I 07 (sections 1–7 in the Example) must be applied.

## 2.2 Management of users and access rights

### 2.2.1 Requirements laid down in the Act on Secondary Use

Section *22 Access rights of the users of the secure operating environment*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P22

### 2.2.2 Requirements imposed by the data permit authority

1. Access rights to the environment are restricted so that users can access only the materials and resources for which they have been granted permit. Access rights to the environment are restricted according to data permits. If a person has more than one data permit in the environment, they can only access materials in one data permit at a time.

2. Access rights to the environment are granted on the principle of least privilege (KATAKRI I 02).

3. Only user IDs from trusted identification sources are used in the environment.

4. If the service provider detects any abuse, it must prevent further damage without delay by restricting access rights, for instance.

5. An access right to the user environment is automatically locked after the data permit has expired.

6. Materials in the user environment will be automatically deleted no later than six (6) months after ~~the~~ access rights have expired, unless otherwise specified by law.

7. In addition to the above, KATAKRI subdivision I 06 (sections 1–10 in the Example) must be applied.

## 2.3 Protecting the environment

### 2.3.1 Requirements laid down in the Act on Secondary Use

*Section 18 General data security requirements* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P18

*Section 23 Protecting the secure operating environment* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P23

*Section 24 Minimum requirements for secure operating environment* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P24

### 2.3.2 Requirements imposed by the data permit authority

1. The access control environment must be protected in accordance with KATAKRI I 01 Protection level IV.

2. The user environment and the quarantine environment must be protected in accordance with KATAKRI I 01 Protection level IV.

3. Details for the requirements:

    a. The user environment is separated from the Internet with a firewall solution.

    b. If a terminal device arranged by the service provider for the user, dedicated for use in the user environment, is located within the same physically and technically protected area as the user environment, two-factor authentication is not required, but the user's identity must be assured before the dedicated terminal device is released for use. The terminal device must not be connected outside the user environment, and the user must not be able to import or export data from the user environment using the terminal device, such as a USB memory.

    c. If the terminal device is not located within the same physically and technically protected area as the user environment, log-in must be implemented by means of two-factor authentication, where the latter step must be implemented before materials can be accessed.

    d. Direct connections from the user's terminal device to the user environment are prohibited. For example, the connection transfers only screen images and input from the keyboard and mouse.

    e. User environments of different data permits must be separated from each other so that only the users mentioned in the data permit in question have access to the data sets concerning the permit.

    f. Users are not granted admin user rights to computers in the operating environment. This is subject to KATAKRI I 06 (sections 1–10 in the Example), in compliance with the Principle of least privilege.

    g. For gateway solutions used between environments at different protection levels, KATAKRI I 01 example sections 1–3 shall apply.

4. In protecting the system, the principle of Minimality and of least privilege in KATAKRI I 08 (sections 1–17 in the Example) shall apply

5. In protecting the system, the principle of Defence-in-depth (KATAKRI I 09, I 13, sections 1–3 in the Example) shall apply.

6. If the controller needs to transfer material subject to a permit, located in its own environment, to its own secure operating environment within the same physically and technically protected area, the transfer may also be carried out without a Secure operating service. Here, KATAKRI subdivision I 15 (Example 2) shall be followed, as applicable.

7. In the management of software vulnerabilities, KATAKRI subdivision I 23 (sections 1–2 in the Example) must be applied.

8. Regular security scans must be performed on the operating environment.

## 2.4 Logs

### 2.4.1 Requirements laid down in the Act on Secondary Use

*Section 19 Data in logs* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P19

### 2.4.2 Requirements imposed by the data permit authority

1. Data in logs must be processed in the same secure way as special category personal data.

2. Usage logs must contain information about the controller that has been granted a data permit, the purpose under the Act on Secondary Use, the user entitled to process data according to the data permit, the data processed, categories of information, and the time of use of the data.

3. Technical log data must be collected comprehensively so that any errors or data breaches can be investigated comprehensively enough. These technical logs must be kept for at least five (5) years.

4. In other respects, KATAKRI I 10 guidelines are applied to logs (sections 1–7 of the Example).

5. Management connections and operations must be protected in accordance with KATAKRI I 04.

6. Logs must be monitored and analysed systematically and regularly.

7. Use of log data must be implemented in such a way that information on viewing is also recorded in the system.

8. Permit-specific usage log data on materials and user registers must be submitted to the data permit authority, at its request, without undue delay.

## 2.5 Management and monitoring of the environment

### 2.5.1 Requirements imposed by the data permit authority

1. The operating environment is documented and the documentation must be available for assessment and other audits carried out by the inspection body.

2. The operating environment must be monitored automatically 24 hours a day.

3. In monitoring of the user environment, special attention must be paid to the monitoring of information security.

4. The KATAKRI I 11 criteria, as applicable, must be used to detect incidents in the operating environment.

5. The validity of the operating environment information security must be monitored and reviewed regularly.

6. Management of the operating environment, in terms of information security, must be done using an encrypted communication connection from a hardened workstation.

7. Maintenance of the operating environment must be carried out from suitable premises.

8. Servers of the operating environment must be located on secure premises, in compliance with the KATAKRI F 01 instructions.

9. Admin user rights for the operating environment must be personal access rights, specifically assigned according to the duties.

10. If necessary, admin user rights to the operating environment must be divided into admin user rights at different levels (Administration Tier Model).

11. Admin user rights to the operating environment are subject to the principle of least privilege in KATAKRI I 06 (sections 1–10 in the Example) and the principle of defence-in-depth in KATAKRI I 07 (sections 1–7 in the Example).

12. In the management and monitoring of the operating environment, KATAKRI subdivisions I 03 and I 04 shall apply, as applicable.

13. In change management of the operating environment, KATAKRI subdivision I 20 (sections 1–3 in the Example) shall apply, as applicable.

14. Actions taken by administrators of the secure operating environment must also be included in log management.

15. If it is suspected that the processing of data violates the law or the terms and conditions of the data permit granted, the service provider must be able to notify the data permit authority without delay and submit a detailed report on the matter. This does not exclude other obligations imposed by legislation.

## 2.6 Removal of materials from the operating environment

### 2.6.1 Requirements imposed by the data permit authority

1. Materials must be removed from the operating environment six (6) months after the end of the data permit, unless otherwise specified in the data permit.

2. KATAKRI I 19 guidelines shall apply to the removal of materials (sections 2 and 3 of the Example).

3. Any conditions set out in the data permit must be taken into account in the storage of materials.

# 3 Reliability of the operator

## 3.1 General information

### 3.1.1 Requirements laid down in the Act on Secondary Use

*Section 20 Secure operating environment* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P20

*Section 25 Demonstrating the data security of the secure operating environment*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P25

*Section 26 Assessment of data security* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P26

*Section 27 Revoking a certificate issued by an assessment body*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P27

*Section 28 Notification obligation of the data security assessment body*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P28

*Section 29 Monitoring of the secure operating environment after deployment*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P29

*Section 30 Supervision of and audits to information systems*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P30

*Section 31 The right of the National Supervisory Authority for Welfare and Health to use external experts* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P31

*Section 32 Right to information of the National Supervisory Authority for Welfare and Health*
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P32

*Section 33 Regulation issued by the National Supervisory Authority for Welfare and Health to correct defects and a penalty payment* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P33

*Section 34 Regulation to fulfill duties* https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P34

### 3.1.2 Requirements imposed by the data permit authority

1. The secure operating environment must be physically located in the EU/EEA.

2. The service provider of the secure operating environment must be an organisation registered in the EU/EEA.

3. It must be possible to assess the reliability of the service provider by applying chapter “Service provision” (p. 12) in the PiTuKri document.

4. The service provider must demonstrate reliability by means of a security management system, for example in accordance with the ISO/IEC 27001 standard.

5. The National Supervisory Authority for Welfare and Health (Valvira) has the right to carry out audits required for supervision. To perform the audit, the auditor has the right to access all premises that engage in the activities referred to in this Act or store information that is relevant to the monitoring of compliance with this Act. This requirement also applies to subcontractors used by the service provider.

## 3.2 Data protection

### 3.2.1 Requirements imposed by the data permit authority

1. A data protection impact assessment (DPIA) in accordance with Article 35 of the EU General Data Protection Regulation (GDPR) must be drawn up on the operating environment.

2. The obligations and agreements concerning the controller and the processor of personal data have been taken into account in accordance with the valid guidelines of the General Data Protection Regulation. The Regulation does not contain instructions, instead it is directly obligatory.

3. The service provider is responsible for ensuring that software, codes or other such products that are transferred to and used in the operating environment and the user environment do not jeopardise the data security of the processing of personal data. In particular, it must be ensured that no personal data is transferred out of the user environment in ways other than as specified for the transfer of materials.

## 3.3 Premises

### 3.3.1 Requirements imposed by the data permit authority

1. Maintenance of the environment must be carried out on premises approved by the information security inspection body.

2. The servers in the environment must be on premises approved by the information security inspection body.

3. As regards security of premises, the physical security audit criteria in KATAKRI F 01-08 shall apply, as applicable.

## 3.4 Personnel

### 3.4.1 Requirements imposed by the data permit authority

A standard security clearance or other similar official report must be completed on persons working in maintenance tasks concerning the operating environment who have access to personal data sets.

1. Employees with access to personal data sets must be familiar with the processing instructions concerning the data sets.

2. As regards personnel safety, KATAKRI subdivisions T 08–12 shall be apply, as applicable.

# 4 Key process steps related to a secure operating environment

| Process step | Tasks | Notes |
|---|---|---|
| Ensuring compliance | The service provider ensures that has a valid certificate on the information security of the operating environment, issued by a information security inspection body. | (Cf. 552/2019, section 25) The certificate must cover all components of the secure operating environment that deal with personal data and components that have an impact on the implementation of personal data protection. |
| | The data permit authority verifies from the public register of the National Supervisory Authority for Welfare and Health that the service provider has a valid certificate. | (Cf. 552/2019, sections 28, 30) |
| | The service provider shall provide the supervisory authority or the party designated by it with an opportunity to monitor compliance with data protection and information security requirements. | (Cf. 552/2019, section 30) |
| | The service provider must store information concerning compliance and other information required for supervision for at least five years after the end of production of the secure operating environment. Usage and disclosure log data must be erased or archived after 12 years have passed from the expiration of the data permit. | (Cf. 552/2019, sections 29, 19) |
| Monitoring and assessment of the secure operating environment | The service provider must maintain an up-to-date and systematic procedure for monitoring and assessing the experiences of using the secure operating environment when it is in production. The service provider must monitor the changes to this Act and correct the operating environment accordingly. | (Cf. 552/2019, section 29) |
| Advice | The service provider offers a service description and a price list of the secure operating environment and advice related to the matter. | The data permit authority provides advisory service only for the secure operating environment it has provided itself. |

| Process step | Tasks | Notes |
|---|---|---|
| Placing an order for the user environment | By means of a procedure arranged by the service provider, the customer places an order from the user environment mentioned in the data permit and encloses the official data permit decision with the necessary appendices to the order. | The service provider gives the customer an opportunity to use electronic services. In addition to the information contained in the permit, key details requested from the customer include:<br>• identifiers of the members of the research group (unique electronic identifiers and identifier federations)<br>• contact details of the members of the research group<br>• the capacity required by the user environment<br>• the software required<br>• billing details. |
| | The service provider verifies the authenticity of an electronically signed data permit. | The data permit has been submitted to the customer in PDF format, signed electronically. |
| | The service provider confirms that the order has been received. | – |
| | The service provider processes the order. | The order must be based on a valid data permit, and the secure operating environment is indicated in the data permit. If necessary, the service provider will request additional information regarding the order from the customer. |
| | The service provider confirms that the order has been processed. | – |
| Establishment of a user environment | Based on the customer's order, the service provider establishes a user environment specific to the data permit. | – |
| | The service provider creates user accounts and access rights for the users mentioned in the permit. | Access and usage rights may only be granted for the duration of the permit to the users mentioned therein. Before opening a connection for the permit holder, the service provider of the operating environment must ensure that the permit holder meets the requirements laid down in the data permit (Cf. 552/2019, section 51) The service provider must maintain a register on users of the secure operating environment and their access rights. The information on the access rights of the users of the operating environment must be erased or archived after 12 years have passed from the expiration of the access right. |

| Process step | Tasks | Notes |
|---|---|---|
| User identification | The identification of users shall comply with the requirements set out in this regulation. | (Cf. 552/2019, section 21 The users of the secure operating environment must be identified reliably and authenticated. Reliable identification can take place, for example, through the Suomi.fi service or a trusted federated identification source. |
| Delivery of login data to users | The service provider shall provide the persons mentioned in the data permit with registration and login instructions, and instructions for activating two-factor authentication. | Any information related to user IDs is provided to the user in a secure manner. |
| Configuration of access rights | The persons mentioned in the data permit are granted access rights to materials subject to a permit. The service provider configures the permit holder's access rights to personal data as well as the access rights of other people who process personal data in the operating environment. | All users of the operating environment must be mentioned in the data permit issued by the data permit authority. Access rights may be valid only for the duration of the permit. The service provider must maintain a register on users of the secure operating environment and their access rights. The information on the access rights of the users of the operating environment must be erased or archived after 12 years have passed from the expiration of the access right. |
| Delivery of materials to the secure environment | As a rule, materials are transferred to the service provider via a secure ~~user~~ operating service. | If the controller needs to transfer material subject to a permit, located in its own environment, to its own secure operating environment within the same physically and technically protected area, the transfer may also be carried out without a secure operating service. |
| | The service provider verifies the integrity and accuracy, as well as information security of the materials it receives. | – |
| | The service provider makes the materials available in the user environment for the users referred to in the permit. | – |
| Transferring finished outputs out of a secure environment | The service provider transfers the customer's finished outputs, via a secure operating service, for verification by the data permit authority with regard to anonymisation. | However, for a justified reason, the data permit authority may, in its permit decision, grant the permit holder the right to implement the anonymisation of the aforementioned information, provided that it is submitted to the data permit authority afterwards. |

| Process step | Tasks | Notes |
|---|---|---|
| Processing and implementation of change orders | The service provider receives change requests and additional orders related to the user environment in accordance with its own service description, and implements them in a documented manner within the framework of the data permit. | If changes ordered by the customer are in conflict with the law or a valid data permit, they may not be implemented. |
| Termination of use of the user environment | The service provider closes users' access to the user environment after the expiry of the validity of the data permit, after the termination of the contract, at the request of the customer or when the authority so orders. | – |
| | The service provider deletes personal data sets in a secure manner, agreeing on the date and time with the customer, but no later than six (6) months after the end of the data permit, unless otherwise provided. | – |